WHAT IS CLAIMED:

1. A method for creating a semi-private peer network, comprising:

in attempting to connect to one or more member peer nodes corresponding to one or more addresses on a connection list of addresses corresponding to member peer nodes of the semi-private peer network, sending an encrypted or otherwise obfuscated key from a connecting member peer node of the semi-private peer network to the one or more member peer nodes; and

establishing a connection between the connecting member peer node and the one or more member peer nodes that successfully decrypt or de-obfuscate the encrypted or otherwise encrypted key.

2. The method of claim 1, wherein addresses are TCP/IP addresses, sending an encrypted or otherwise obfuscated key comprises sending a packet with the encrypted or otherwise obfuscated key and establishing a connection comprises establishing a connection upon receiving an acknowledgement from the one or more member peer nodes that successfully decrypt or de-obfuscate the encrypted or otherwise encrypted key.

3. The method of claim 2, wherein the connection list further includes TCP port identifiers associated with the TCP/IP addresses, to designate the port on which a member peer node corresponding to a TCP/IP address handles semi-private network traffic and sending a packet comprises sending a packet to the one or more TCP ports associated with the one or more member peer nodes.

4. The method of claim 1, wherein the connection list further includes one or more encrypted or otherwise obfuscated keys associated with the one or more addresses on the connection list.

5. The method of claim 1, wherein establishing a connection comprises limiting establishing a connection to the one or more member peer nodes that are not connected to a same set of member peer nodes as an already connected member peer node.

6. A computer program product including computer program code to cause a microprocessor to perform a method for creating a semi-private peer network, the method comprising:

in attempting to connect to one or more member peer nodes corresponding to one or more addresses on a connection list of addresses corresponding to member peer nodes of the semi-private peer network, sending an encrypted or otherwise obfuscated key from a connecting member peer node of the semi-private peer network to the one or more member peer nodes; and

establishing a connection between the connecting member peer node and the one or more member peer nodes that successfully decrypt or de-obfuscate the encrypted or otherwise encrypted key.

7. The computer program product of claim 6, wherein addresses are TCP/IP addresses, sending an encrypted or otherwise obfuscated key comprises sending a packet with the encrypted or otherwise obfuscated key and establishing a connection comprises establishing a connection upon receiving an acknowledgement from the one or more member peer nodes that successfully decrypt or de-obfuscate the encrypted or otherwise encrypted key.

8. The computer program product of claim 7, wherein the connection list further includes TCP port identifiers associated with the TCP/IP addresses, to designate the port on which a member peer node corresponding to a TCP/IP address handles semi-private network traffic and sending a packet comprises sending a packet to the one or more TCP ports associated with the one or more member peer nodes.

9. The computer program product of claim 6, wherein the connection list further includes one or more encrypted or otherwise obfuscated keys associated with the one or more addresses on the connection list.

10. The computer program product of claim 6, wherein establishing a connection comprises limiting establishing a connection to the one or more member peer nodes that are not connected to a same set of member peer nodes as an already connected member peer node.

11. A member peer node of a semi-private network, comprising:

a connection list of addresses corresponding to member peer nodes of the semi-private peer network; and

a semi-private peer network application to, in attempting to connect to one or more member peer nodes corresponding to one or more addresses of the connection list, send an encrypted or otherwise obfuscated key to the one or more member peer nodes for decryption or de-obfuscation by the one or more member peer nodes, and to decrypt or de-obfuscate an encrypted or otherwise obfuscated key sent by one or more member peer nodes of the semi-private peer network attempting to connect with the member peer nodes.

12. The member peer node of claim 11, wherein addresses are TCP/IP addresses, sending an encrypted or otherwise obfuscated key comprises sending a packet with the encrypted or otherwise obfuscated key and establishing a connection comprises establishing a connection upon receiving an acknowledgement from the one or more member peer nodes that successfully decrypt or de-obfuscate the encrypted or otherwise encrypted key.

13. The member peer node of claim 12, wherein the connection list further includes TCP port identifiers associated with the TCP/IP addresses, to designate the port on which a member peer node corresponding to a TCP/IP address handles semi-private network traffic and sending a packet comprises sending a packet to the one or more TCP ports associated with the one or more member peer nodes.

14. The member peer node of claim 11, wherein the connection list further includes one or more encrypted or otherwise obfuscated keys associated with the one or more addresses on the connection list.

15. A bridging agent for connecting a semi-private peer network to another network, comprising:

an examination unit that examines requests and/or queries circulating within the semi-private peer network and/or another network; and

an insertion unit that inserts one or more of the requests and/or queries within the semi-private peer network into the another network and/or inserts one or more of the requests and/or queries within the another network into the semi-private network, when the requests

and/or queries are determined appropriate by the bridging agent for circulation within the another network and/or semi-private peer network respectively.

16. The bridging agent of claim 15, wherein the another network is another semi-private peer network.

17. The bridging agent of claim 15, wherein the bridging agent has a member status within the semi-private peer network and the another network so as to allow the bridging agent permission to monitor, initiate and respond to request and/or queries in the semi-private peer network and/or another network.

18. The bridging agent of claim 15, wherein the requests and/or queries are determined appropriate for circulation within the another network and/or semi-private peer network through the use of high-level criteria to assess if the requests and/or queries comprise information that sufficiently overlaps with or is relevant to the subject matter or interest of the semi-private peer network and/or another network.

19. The bridging agent of claim 15, wherein inserting one or more requests and/or queries comprises copying one or more packets associated with the one or more requests and/or queries and injecting the one or more packets into the semi-private network and/or another network to which the one or more requests and/or queries are inserted.

20. The bridging agent of claim 15, wherein inserting one or more requests and/or queries comprises creating one or more new packets corresponding to the one or more requests and/or queries and circulating the one or more new packets into the semi-private network and/or another network to which the one or more requests and/or queries are inserted.

21. A method for bridging a semi-private peer network to another network, comprising:

examining requests and/or queries circulating within the semi-private peer network and/or another network; and

inserting one or more of the requests and/or queries within the semi-private peer network into the another network and/or inserting one or more of the requests and/or queries

within the another network into the semi-private network, when the requests and/or queries are determined appropriate by the bridging agent for circulation within the another network and/or semi-private peer network respectively.

22. The bridging agent of claim 21, wherein the another network is another semi-private peer network.

23. The bridging agent of claim 21, wherein examining the requests and/or queries comprises having a member status within the semi-private peer network and the another network so as to allow for monitoring, initiating and responding to request and/or queries in the semi-private peer network and/or another network.

24. The bridging agent of claim 21, wherein the requests and/or queries are determined appropriate for circulation within the another network and/or semi-private peer network through the use of high-level criteria to assess if the requests and/or queries comprise information that sufficiently overlaps with or is relevant to the subject matter or interest of the semi-private peer network and/or another network.

25. The bridging agent of claim 21, wherein inserting one or more requests and/or queries comprises copying one or more packets associated with the one or more requests and/or queries and injecting the one or more packets into the semi-private network and/or another network to which the one or more requests and/or queries are inserted.

26. The bridging agent of claim 21, wherein inserting one or more requests and/or queries comprises creating one or more new packets corresponding to the one or more requests and/or queries and circulating the one or more new packets into the semi-private network and/or another network to which the one or more requests and/or queries are inserted.